Nepal Stock Exchange

IT Audit Guidelines for Trading Members

January 2026

TABLE OF CONTENTS

कम्पनी सचिव

LIST OF ABBREVIATIONS

DC	Data Center
DRC	Disaster Recovery Center
IS	Information System
ISO	International Organization for Standardization
ICT	Information and Communication Technologies
IT	Information technology
IP	Internet protocol
NEPSE	Nepal Stock Exchange
PPMO	Public Procurement Monitoring Office
RBAC	Role Based Access Control
SEBON	Securities Board of Nepal
SOP	Standard Operating Procedure
TMS	Trade Management System
ToR	Terms of Reference
UAT	User Acceptance Test

1. Introduction

Nepal Stock Exchange (NEPSE) acknowledges the vital role of a secure and resilient information technology infrastructure in today's financial services environment. As trading members increasingly rely on digital platforms for trading, settlement, and client data management, safeguarding the integrity, confidentiality, and availability of information systems has become critical. Recognizing this, NEPSE has developed these IT Audit Guidelines to provide trading members with a structured and comprehensive approach to evaluating their IT environments. The guidelines serve as a practical tool to help trading members identify potential risks, implement appropriate controls, and strengthen their cybersecurity posture in alignment with industry best practices.

The primary objective of these guidelines is to establish a standardized framework for conducting Information Systems (IS) audits across trading members firms. By following this framework, brokers can ensure regulatory compliance, protect sensitive client and business data, and maintain operational resilience. In addition, the guidelines promote continuous improvement in IT governance, risk management, and security practices, thereby fostering trust and confidence among stakeholders in Nepal's capital market ecosystem. This IT Audit Guidelines has been formulated in accordance with the *NEPSE Trading Operations Bylaw, 2079 (Fourth Amendment) (Clause No: 21 (Ta))*, ensuring alignment with the regulatory framework and industry best practices.

2. Objectives

The primary objectives of these guidelines are to:

a) Establish a clear framework for conducting periodic and comprehensive IT audits.

b) Ensure the confidentiality, integrity, and availability of all trading and client information.

c) Assess the effectiveness of IT controls and security measures.

d) Identify and mitigate potential IT risks and vulnerabilities.

e) Ensure compliance with regulatory requirements and industry best practices.

f) Improve the overall IT governance and management within the brokerage firm.

3. Applicability of the Guidelines

The IT Audit Guidelines are applicable to all trading member's information systems and IT infrastructure used by them in the course of their operations. This includes, but is not limited to, Trade management System (TMS), Broker Back Office System, client data management systems, network and communication infrastructure, servers, databases, and storage systems. The guidelines also cover websites, mobile applications, and related digital platforms, as well as business continuity and disaster recovery plans. By applying these guidelines across all relevant

IT assets, trading members can ensure comprehensive assessment, risk mitigation, and compliance with regulatory and industry best practices.

The system auditor shall verify at least following features of TMS as per the trading bylaws:

a) Order routing, confirmation, modification, cancelation and order status
b) Order history and order records
c) Different types of valid order attributes
d) Order quantity and price limit
e) Trade management, trade confirmation and trade reporting
f) Trading Limits and collateral management
g) Client Verification
h) Client account types
i) Client onboarding and KYC verification process
j) User management
k) Password security and access control
l) Session management
m) Login track records
n) Log management

4. IT Audit Framework

The audit shall be conducted based on the following key domains. Each domain requires a detailed review and assessment of controls and processes.

4.1. Governance and IT Management

a) Review IT governance structure, policies, and roles.

b) Verify IT strategy alignment with business objectives.

c) Verify that clear roles and responsibilities are defined and established.

d) Assess IT risk management practices.

e) Check procedures for IT asset management and change management.

4.2. IT Infrastructure and Network Security

a) Review network architecture, firewalls, and access controls.

b) Assess physical security of servers, data centers, and communication devices.

c) Examine network monitoring and intrusion detection systems.

d) Evaluate patch management, vulnerability assessments, and malware protection.

4.3. Application and Trading System Audit

a) Evaluate the security and functionality of trading and back-office applications.

b) Review authentication mechanisms, authorization controls, and audit logs.

c) Verify segregation of duties in critical applications.

d) Test for potential data breaches, unauthorized access, detect and mitigate malicious automated traffic and system vulnerabilities.

4.4. Data Management and Security

a) Assess data classification, storage, and encryption practices.

b) Review data backup, retention, and recovery mechanisms.

c) Verify data integrity, accuracy, and completeness.

d) Ensure compliance with personal data protection regulations.

4.5. Cybersecurity Policies and Practices

a) Examine the existence and implementation of cybersecurity policies.

b) Check employee/customer awareness and training programs.

c) Evaluate incident management and reporting mechanisms.

d) Assess vulnerability assessment, penetration testing, and threat monitoring practices.

4.6. Regulatory Compliance

a) Review adherence to NEPSE rules, Securities Board of Nepal (SEBON) regulations, and other applicable laws.

b) Ensure timely reporting of IT incidents and breaches.

c) Verify maintenance of audit trails and records for inspection by regulators.

d) Review of the collateral practices for clients.

4.7. Business Continuity and Disaster Recovery

a) Review the existence of disaster recovery and business continuity plans.

b) Test backup restoration and system failover procedures.

c) Evaluate periodic review and update of contingency plans.

कम्पनी

4.8. Others

Except for the domains specified above, trading members shall be required to conduct Information Systems (IS) audits in full compliance with the directives and requirements provided by NEPSE and SEBON .

The detailed audit checklist attached in ***Annex I*** shall be followed to conduct IS Audit of the trading members

5. Audit Process

a) Planning and Preparation: Define audit objectives, scope, and methodology.

b) Information Gathering: Collect IT policies Standard Operating Procedures (SOPs), network diagrams, system documentation, and logs.

c) Risk Assessment: Identify critical assets, threats, and vulnerabilities.

d) Audit Testing: Perform controls testing, vulnerability scans, and compliance checks.

e) Reporting: Document findings, risk rating, and recommendations.

f) Follow-up: Track remediation of audit findings and corrective actions.

कम्पनी सचि

6. Audit Reporting

a) The audit report should include:
   i. Executive summary
   ii. Scope and methodology
   iii. Findings and risk assessment
   iv. Recommendations and action plans
   v. Management responses with timelines

b) All trading members shall carry out an Information Systems Audit at regular intervals, at least once every two years, and submit the audit report within the second quarter of the relevant fiscal year.

c) Newly registered trading members shall conduct their first IS Audit and submit the corresponding audit report within six months of commencement of operations.

d) All existing trading members shall conduct the IS audit and submit the corresponding audit report within six months of commencement of this guideline.

e) In the event of any major system upgrade or significant change to the IT infrastructure, an IS Audit shall be conducted and audit report submitted within the same year of such upgradation.

f) NEPSE shall periodically review the Terms of Reference (ToR) of system audit, if required.

g) Failure to comply with this guideline shall be subjected to disciplinary actions according to prevailing rules and regulations.

7. Eligibility Criteria for the Information System Audit

The eligibility criteria for conducting an Information Systems Audit of trading members are outlined and explained in detail below, defining the minimum qualifications, competencies, and requirements that must be met to ensure a thorough, independent, and standards-based audit process.

a) The consulting firm shall be registered in the respective country.

b) The consulting firm shall have a tax clearance certificate of previous fiscal year (for Domestic Consulting Firms).

c) The consulting firm shall not be blacklisted by Public Procurement Monitoring Office (PPMO).

d) The consulting firm should have completed at least one Information System Audit project or assignment for an organization in the banking, insurance, financial institution, capital market, or government sector.

कम्पनी सचिव

e) The consulting firm must engage at least three (3) system audit professionals including

Designation	Qualification	Experience
Information Security Expert	Bachelor's in IT with relevant certification like CISA/CISM/CISSP/OSCP/CPTE/LPT/ CEH/CRISC/Security+ or similar.	Minimum 5 years of specific work experience in the related field
Vulnerability assessor / Ethical Hacker/ Application Security Engineer/ Threat Analyst	Bachelor's Degree in IT related field	Minimum 2 years of specific work experience in the related field.

f) The Auditor shall not have any conflict of interest in conducting fair, objective and independent audit of the trading member.

कम्पनी सचिव

Annex I: Information System Audit Checklist

1	Organizational Controls	Observations
1.1	Policies for Information Security	
1.2	Information Security Roles and Responsibilities	
1.3	Segregation of Duties	
1.4	Management responsibilities	
1.5	Contact with Authorities	
1.6	Contact with Special Interest Group	
1.7	Threat Intelligence	
1.8	Information Security in Project Management	
1.9	Inventory of Information and other associated assets	
1.10	Acceptable use of Information and other associated assets	
1.11	Return of Assets	
1.12	Classification of Information	
1.13	Labelling of Information	
1.14	Information Transfer	
1.15	Access Control	
1.16	Identity Management	
1.17	Authentication Information	
1.18	Access Rights	
1.19	Information Security in Supplier Relationships	
1.20	Addressing Information Security within Supplier Agreements	
1.21	Managing Information Security in the ICT Supply Chain	
1.22	Monitoring, Review and Change Management of Supplier Services	
1.23	Information Security for use of Cloud Services	
1.24	Information Security Incident Management Planning and Preparation	
1.25	Assessment and decisions on Information Security Events	
1.26	Response to Information Security Incidents	
1.27	Learning from Information Security Incidents	
1.28	Collection of evidence	
1.29	Information Security during Disruption	
1.30	ICT Readiness for Business Continuity	
1.31	Legal, Statutory, Regulatory and Contractual Requirements	
1.32	Intellectual Property Rights	
1.33	Protection of Records	
1.34	Privacy and Protection of Personal Identifiable Information (PII)	
1.35	Independent Review of Information Security	
1.36	Compliance with Policies, Rules and Standards for Information Security	
1.37	Documented Operating Procedures	

2	People Controls	
2.1	Screening	
2.2	Terms and Conditions of Employment	
2.3	Information Security Awareness Education and Training	
2.4	Disciplinary Process	
2.5	Responsibilities after Termination or Change of Employment	
2.6	Confidentiality or Non-Disclosure Agreements	
2.7	Remote Working	
2.8	Information Security Event Reporting	
3	Physical Controls	
3.1	Physical Security Perimeters	
3.2	Physical Entry	
3.3	Securing Offices, Rooms and Facilities	
3.4	Physical Security Monitoring	
3.5	Protecting against Physical and Environmental Threats	
3.6	Working in Secure Areas	
3.7	Clear Desk and Clear Screen	
3.8	Equipment Siting and Protection	
3.9	Security of Assets Off-Premises	
3.10	Storage Media	
3.11	Supporting Utilities	
3.12	Cabling Security	
3.13	Equipment Maintenance	
3.14	Secure Disposal and Re-use of Equipment	
4	Technological Control	
4.1	User and Point Devices	
4.2	Privileged Access Rights	
4.3	Information Access Restrictions	
4.4	Access to Source Code	
4.5	Secure Authentication	
4.6	Capacity Management	
4.7	Protection against Malware	
4.8	Management of Technical Vulnerabilities	
4.9	Configuration Management	
4.10	Information Deletion	
4.11	Data Masking	
4.12	Data Leakage Prevention	
4.13	Information Backup	
4.14	Redundancy of Information Processing Facilities	
4.15	Logging	
4.16	Monitoring Activities	
4.17	Clock Synchronization	
4.18	Use of Privileged Utility Programs	

कम्पनी सचिव

4.19	Installation of Software on Operational Systems	
4.20	Networks Security	
4.21	Security of Network Services	
4.22	Segregation of Networks	
4.23	Web Filtering	
4.24	Use of Cryptography	
4.25	Secure Development Life Cycle	
4.26	Applications Security Requirements	
4.27	Secure System Architecture and Engineering Principles	
4.28	Secure Coding	
4.29	Security Testing in Development and Acceptance	
4.30	Outsourced Development	
4.31	Separation of Development, Test and Production Environments	
4.32	Change Management	
4.33	Test Information	
4.34	Protection of Information System during Audit Testing	